BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 12/46

A1

(11) International Publication Number: WO 98/19425

(43) International Publication Date: 7 May 1998 (07.05.98)

(21) International Application Number: PCT/US97/19523

(22) International Filing Date: 29 October 1997 (29.10.97)

(30) Priority Data:
08/739,360 29 October 1996 (29.10.96) US

(71) Applicant: MCI COMMUNICATIONS CORPORATION [US/US]; 1133 19th Street, N.W., Washington, DC 20036 (US).

(71)(72) Applicant and Inventor: PURVIS, Scott, G. [US/US]; Apartment 1074, 1616 Blue Danube, Arlington, TX 76015 (US).

(74) Agents: WARREN, Sanford, E., Jr. et al.; Warren & Perez, Suite 710, 8411 Preston Road, Dallas, TX 75225 (US).

(81) Designated States: AU, CA, JP, MX, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: METHOD AND ARCHITECTURE FOR A WIDE AREA NETWORK

(57) Abstract

An architecture for a wide area network offering many of the advantages of the Internet but is easily modified to accommodate changes in network growth or demand is disclosed. The architecture includes a redundant high speed dual switched Ethernet backbone which is designated as Area 0 in the network topology. Area Border Routers (ABRs) are linked to the backbone and provide a gateway to a Core Network Service which consists of a plurality of network routers and switches. The ABRs are also linked to more regional routers which are geographically located in critical areas of interest across the network. The architecture accommodates devices and applications using the Internet Protocol, Domain Name Server addresses and other industry standard addressing and naming formats and includes a security architecture for validating authorized users.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND ARCHITECTURE FOR A WIDE AREA NETWORK

TECHNICAL FIELD

The invention relates in general to a data network architecture, and, more particularly to wide area network infrastructure that facilitates centralized reconfiguration of network resources to accommodate network growth and expansion.

BACKGROUND OF THE INVENTION

The Internet has become the information "superhighway" of choice for an ever increasing number of individuals who have turned to it as an inexpensive and effective way of exchanging electronic data and information. While often thought of as a world-wide network, in reality the Internet is comprised of numerous different networks throughout the world which are linked together using a common routing protocol (the Internet Protocol (IP)). Thus, no single controlling entity manages Internet traffic on a network wide basis.

The Internet has acquired universal appeal by providing widespread access from an unspecified number of terminals or other dial-in equipment around the world. Individual users, groups and other entities are identified on the Internet by a unique address conforming to the IP. A local access hub provides users with an entry point into the Internet network. The local hub acts as the exchange point for both incoming and outgoing data by routing messages to their intended recipients. Since a point-to-point connection is never established, the costs are limited to those charged by the local access provider and/or a nominal periodic access fee.

While the flexibility, ease of access and low cost associated with Internet use have attracted many, the wide open architecture has some inherent limitations. First, hardware and application upgrades cannot be effected on a network wide basis from a single location. Instead, each local must be individually upgraded at the appropriate level along the network hierarchy meaning that network upgrades and enhancements can be time consuming and expensive.

Another limitation of the Internet as well as other types of Wide Area Networks (WANs) is the impact that an upgrade or change may have on other systems in the network hierarchy. Most WANS use a linear transmission channel topology wherein data traffic is routed from one point to the next based on a routing protocol which determines the best path between the two points. The end-to-end transmission, however, may comprise dozens of points along a Switched Virtual Channel (SVC) meaning that the best end-to-end route may not be selected.

In addition, the impact to data flow during times of heavy traffic may result in bottlenecks which limit network throughput and increase system response times. While methods and systems of monitoring and rerouting data traffic are available, the rapid growth and phenomenal popularity of WANs such as the Internet have made a system wide redesign an expensive and complicated proposition. In addition, the manpower and time requirements associated with scaling a WAN to implement network upgrades are in most instances prohibitive.

What is needed is a network architecture that offers many of the benefits of existing WANs but is easily modified to accommodate changes in network growth with time.

SUMMARY OF THE INVENTION

It has been found that network wide reconfiguration of existing WANs is too costly and in many instances requires a massive overhaul of existing software and hardware systems within the network topology.

Accordingly, it is a primary object of the present invention to provide an improved network architecture suitable for a WAN implementation that provides centralized reconfiguration of network resources. In this regard, a three-tier hierarchy is provided that defines an Area 0 signal path for routing network traffic via a plurality of centrally located network components. A dual switched Ethernet link or localized media connection such as FDDI, token ring, ATM, etc. ... may be used as the exchange link and supports a plurality of routers which are located in geographic areas of interest according to network demands.

Another object of the present invention is to provide a network topology that is highly scalable and accommodates increases in network resources. In this regard, the core network components may be upgraded and expanded at a single facility using commercial off-the-shelf (COTS) components. Device and application addresses may be assigned according to accepted industry protocols and the assigned addresses and names updated to provide additional network bandwidth without a complete overhaul of existing applications.

Yet another object of the present invention is to provide a network architecture that is resilient and tolerant of interruptions and faults that occur along data traffic channels. In this regard, redundant communications links are used and load balanced during

normal operation, with enough channel bandwidth provided so a channel can sustain network traffic should one channel fail. The switched Ethernet backbone is used to provide a redundant connection for the various system routers across the network.

For a more complete understanding of the present invention, including its features and advantages, reference is now made to the following detailed description, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings:

Figure 1 is a block diagram of an architecture for a prior art wide area network;

Figure 2 is a block diagram illustrating the network architecture for an improved wide area network according to one embodiment of the invention;

Figure 3 is a block diagram illustrating the connectivity of the routing components to the Core Network according to one embodiment of the invention;

Figure 4 is a block diagram showing the interface between an existing routed data network and the Core Network according to one embodiment of the invention;

Figure 5 is a detailed connectivity and signal protocol diagram according to one embodiment of the invention;

Figure 6 is a connectivity diagram showing the signal pathways between separate areas via the switched Ethernet backbone and the core network;

Figure 7 is a block diagram showing the Internet Protocol (IP) administration features according to one embodiment of the invention;

Figure 8 is a flow diagram of the addressing and name assignment process according to one embodiment of the invention;

Figure 9 is a block diagram showing the Domain Name Server update flow according to one embodiment of the invention;

Figure 10 is a flow diagram for the network security architecture according to one embodiment of the invention; and

Figure 11 is a block diagram of a cabinet

configuration of the various network components according to one embodiment.

Corresponding numerals refer to corresponding parts in the figures unless otherwise indicated.

5

DETAILED DESCRIPTION OF THE INVENTION

In Figure 1, a network architecture for a prior art Wide Area Network (WAN) is shown and denoted generally as 10. Network architecture 10 has regional hubs 15, 17, 19 and 21 which form an upper level 25 (Level I) of the network hierarchy and are communicably linked to one another via channels 16, 18, 20 and 22. In practice, the regional hubs 15, 17, 19 and 21 are physical locations of a data bearing network at which the various routing and switching components are located.

The channels 16, 18, 20 and 22 comprise data signal paths which connect the various subsystems allowing a point-to-point transmission of digital data using industry standard protocols. The router and switching devices as well as the signal protocols are well known to those skilled in the art.

At downstream level 40 (Level II), hubs 30, 32, 34 and 36 provide more localized distribution points along the network architecture 10. Since no single controlling entity is used at the higher level 25, data traffic is routed at each point before reaching a localized hub 30, 32, 34 or 36 using a preestablished routing protocol such as Open Shortest Path First (OSPF) or similar routing scheme. As is understood by those skilled in the art, the logical signal pathways which form the Level I 25 to Level II hierarchy of architecture 10 defines the "Area 0" signal path.

A lower level 50 (Level III) on the network hierarchy is shown comprising points 42, 44, 46 and 48. Thus, signal path flow from a one point, for example 48, to a second point 42, is routed via area hub 36 into regional hub 21 as an entry point into the Area 0 wherein

it is routed using one or more virtual channels conforming to established signaling protocols before reaching hub 30 and being routed to point 42.

The network architecture 10 of Figure 1 has inherent limitations. Since the signal routing functions are distributed across the network, upgrades and network maintenance must occur at a plurality of physically distant cites along the network hierarchy. Increasing the available network bandwidth becomes a massive undertaking which may compromise network integrity. Thus, the infrastructure of network architecture 10 is not easily changed or augmented to accommodate network resource requirements.

Turning now to Figure 2, an improved network architecture according to the invention is shown and denoted generally as 75. Area border hubs 80, 82, 84 and 86 are communicably linked to one another via core 88 and channels 81, 83, 85 and 87. The core 88 comprises various switching and routing devices as herein described, although a primary feature of the core 88 is its scalability which permits quick and easy reconfiguration by making physical changes at the core 88 level. In one embodiment, the core 88 components are rack mounted at a single physical facility.

As shown, the area border hubs 80, 82, 84 and 86 are, in turn, linked to backbone 90 via paths 92, 94, 96 and 98. In one embodiment, the backbone 90 is configured as an switched Ethernet topology which permits high speed data transfers although other localized mediums may be used. The arrangement of backbone 90 is particularly advantageous providing an Area 0 OSPF pathway between levels 25 and 40 of network architecture 75.

Regional hubs 100 are coupled to backbone 90 as shown and located at geographic locations and areas of interest according to traffic demands. As such, the number and location of regional hubs 100 may vary to accommodate network wide demands. As is appreciated by those skilled in the art, the Ethernet backbone topology 90 provides the communications channels to higher levels on the network hierarchy, meaning a reconfiguration at core 88 will have system wide effect. Thus, expanding network bandwidth entails reconfiguring the components of core 88 and modifying the address and naming schemes at the core 88.

The core 88 components can be maintained at a single facility (see Figure 11). In this way, a network hierarchy that can be easily changed or augmented to accommodate network requirements is defined. Lower levels 105 of the network architecture 75 are communicably linked to upper levels 100 via well known methods.

Turning to Figure 3, the connectivity scheme to the core 88 network components is shown wherein a plurality of routers 110, 112, 114 and 116 are communicably linked to the core 88 network service via service paths 120 and 122. As shown in Figure 3 and according to one preferred embodiment, the service paths 120, 122 are joined by multiplexers 125 and 130 which comprise gateways into the router 110 and core 88, respectively.

Various component devices may be used as multiplexers 125 or 130, although a Digital Link (DL) 3800 T-1 inverse multiplexer has been found suitable. Also, the access service paths 120 and 122 can comprise high speed T-1 links capable of carrying traffic at over

4 Mbps. The service paths 120, 122 can be arranged for load sharing wherein both paths carry data traffic under normal conditions. Alternatively, the service paths 120 and 122 may be arranged and configured to independently carry the data router 110 traffic in the event of failure by either one of the service paths 120, 122. In this way, a local level of redundancy and resiliency is provided.

According to one embodiment, the core 88 network can comprise the HyperStream Frame Relay Network service known to those skilled in the art. If so, each of the two service paths 120 and 122 can provide fully meshed access via routers, such as 112, 114 or 116, and permanently virtual circuits provisions on the HyperStream Frame Relay Network. Also in one embodiment, the Border Gateway Protocol version 4 (BGP-4) can be used for communications between the core network 88 using OSPF interior gateway protocol.

An advantage of the present network architecture according to the invention is its inter-operability and connectivity to existing data networks. These features are illustrated in Figure 4 which illustrates the interface between the improved architecture 75 and an existing data network 150.

A plurality of routers 110, 112, 114 are communicably linked to the core network 88 as herein described and provide an access pathway to a pair of dual horned gateway routers 155 and 160. Switched Ethernet backbone segments 90 provide the signal paths between the dual horned routers 155 and 160 to route existing router devices 165 and 170, respectively. The dual horned gateway router arrangements 155 and 160 provide four

direct paths into the core network 88 with multiple levels of router and connection diversity.

As shown, the existing network routers 165 and 170 provide gateways into the prior data network 150 via high speed T-1 links 175 and 180, respectively. While Figure 4 shows the interface of the improved network architecture 75 at two distinct points 165, 170, it should be understood that less or more connection points may be achieved by adding or subtracting router and connections segments in like fashion.

In Figure 5, a detailed connection and protocol diagram is shown according to one embodiment of the invention. An existing data network 200 is coupled to an autonomous system server 205 which correlates the various network data routing and switching functions assuring data traffic is load-balanced throughout the network. A 4 Mbps transport link 203 connects the existing data network components 200 to the autonomous system server. Likewise, high speed transport links connect the autonomous system server to autonomous system border routers 207 and 209 (ASBR). The configuration provides a dual gateway path into the core network server 205.

In one embodiment, the ASBRs 207, 209 are Cisco Series 4700 routers running Cisco Rev. 11.0 software and providing 2 x 4.5 Mbps per second dual links to the core access server 205. It should be understood, however, that other similar device types may be employed. As shown, a dial-up server 211 is provided and coupled to the ASBR devices 207, 209 to provide support for various dial-up services including a remote system use.

The ASBR components 207, 209 provide a tie into area border routers 215 via the switched Ethernet topology 213

which comprises a high speed switched dual line signal pathway. It is the backbone 213 that provides the Area 0 component of the improved network architecture according to the present invention and links the various ABRs 215 to the core network 205 via ASBRs 207, 209.

In one embodiment, the dual switched Ethernet topology is used 213 and provides two distinct levels of backup. First, if any one port of an ABR device 215 fails, the second port will automatically take over. Second, in the event one of the Ethernet paths 213 fails, the second Ethernet path 213 will automatically handle all backbone traffic until the first path is restored and load balanced.

A backup routing connection is provided via backup router 217 in case any of the ABR devices should fail. This provides an extra level of resiliency and fault tolerance throughout the network. The individual area border routers 215 are located at distinct and separate geographical locations depending on traffic load and network demands.

An advantageous feature of the configuration shown in Figure 5 is the ability to add additional ABRs to accommodate expansion and growth for new data traffic locations by connection to the switched Ethernet topology 213. In this regard, since the autonomous system server 205 is transparently interconnected to the ABR devices via backbone 213, a network-wide modification or upgrade is unnecessary. In this way, network expansion and maintenance is facilitated at a single centralized location.

As shown, the area border routers 215 are communicably linked to a plurality of geographically

distinct area routers 220 which support the OSPF protocol.

It should be understood that the configurations shown are described in connection with a single preferred embodiment and, as such, various components devices and applications may be employed to achieve the advantages of the invention. In one contemplated use of the improved network architecture 75, a plurality of autonomous systems at different physical locations are linked to form a wide area network infrastructure using a plurality of routers, system border routers, area border routers, backup routers, servers, modems, and other systems to create a virtual point of presence (POP) for each location. These POPs can be located in major cities near key facilities to create a network infrastructure that minimizes transit delays and facilitates network and service technology enhancements.

Table 1 below lists various equipment types that can be used to create the network infrastructure based on the POP location type in accordance with one embodiment. As stated, the equipment used may vary according to various contemplated embodiments.

TABLE 1: Network Equipment for POP Type

POP Type	Equipment Brand/Model	Software Version	Access Type
Small Dial-Up Associate Office	Cisco 1601, Microcom V.34 modem	Cisco Rev 11.0 Microcom Ver 1.309	28.8 kbps PPP

Large Associate Office	Cisco 2507 with Ethernet ports; Cray DSUs	Cisco Rev 11.0 Cray Ver 2.01 & 3.13	56 kbps with frame relay CIR = 32 kbps
Process & Distribution Center	Dual Cisco 2518s, Cray DSUs	Cisco Rev 11.0 Cray Ver 2.01	2 x 56 kbps with frame relay CIR = kbps
District Office	Dual Cisco 2524s, Cray CSU/DSUs	Cisco Rev 11.0 Cray Ver 2.0.02	2 x 384 kbps with frame relay CIR = 192 kbps
Data Center	Dual Cisco 4700s, Digital Link DL3800s	Cisco Rev 11.0 Cray DL 1.07.03	2 x 4.5 Mbps dual links to the Core
PVP OSPF Backbone ABR/ASBR	Cisco 4700s, Digital Link DL3800s	Cisco Rev 11.0 DL 1.07.03	Switched Ethernets (Cisco Catalyst 1900)
Core Transport	9 Cisco 4700s, Digital Link DL 3800s	Cisco Rev 11.0 DL 1.07.03	N x T1, frame relay fully meshed

Turning now to Figure 6, a network architecture illustrating the connectivity scheme to distant POP locations is shown. As shown, two distant and distinct area 245 and 270 are communicably linked to each other and to core systems 280 and 282 via the core network 88. One or more POP offices, such as district office 250 and associate office 252 may be linked to a localized frame relay network 260 via paths 254 and 256, respectively. The paths 254 and 256 may be configured as dedicated 56

Kbps frame relay lines in a load-sharing arrangement. In addition, redundancy may be provided between the offices 250, 252 using alternate permanent virtual circuits or switch dial backup channels.

In one embodiment, the frame relay network 260 is used and linked to the ASBR 265 which provides an entry point into the core network 88 via a highspeed 4 Mbps transport access service path 272. An advantage of the present invention lies in the arrangement of the switched Ethernet topology 213 which connects ASBR 265 to ASBR 268 at a distant location corresponding to Area 270.

Area 270 is similarly configured to Area 245 with a high speed transport line 274 used as an entry point into the core network 88. In one embodiment, the core network 88 comprises a framed relay service network known to those skilled in the art. Also the core network 88 may employ a variety of primary and backup transport channels providing redundant signal paths to the core router components 280 and 282. This provides a point-to-point signal pathway between the area routers 265, 268 and the core routers 280, 282.

Because the switched Ethernet topology 213 will support additional router devices, modifications to the overall network can be made without affecting lower

levels of the network hierarchy. Standardized addressing and naming conventions can be used to ensure uniform routing of network frame data to their intended destination.

As such, a uniform addressing and naming scheme has been adopted in conjunction with one embodiment of the invention. In reference to Figure 7, an Internet protocol (IP) address management system that forms part of the invention is shown and denoted generally as 300. An IP administrator 305 is interspersed between a mixed protocol environment having of a plurality of independent and distinct platform types 310. The administrator 305 provides a user-controlled interface that allows the network-wide management of individual system names and addresses for a various server types across the network.

As shown, an IP management tool 315 is operably coupled to the IP administrator 305 and provides a dynamic network configuration tool to map messages, names and addresses from different or similar systems across the network. In one embodiment, the IP manager 310 maps object names to IP addresses and manages a dynamic host configuration protocol (DHCP) 315, domain name service (DNS) 320 and a boot protocol (Bootp) 325. It should be understood that other similar and related IP management

functions may be provided all within the scope of the invention.

As stated, a function of the IP management system 310 is to ensure that every IP capable device or application that is addressable on the network is provided with a unique name for proper routing to its intended designation. As such, and according to one embodiment, the following IP format can be used:

ccccssffaaa.ss.usps.gov

Where:

cccc	denotes a four-character string city name and the device location
ss	denotes a standard two-character state designation
ff	denotes a two-character function code to identify the device
aaa	denotes a unique alphanumeric identifier setup by the NNSC

Other conventions may be adopted, all within the scope of the present invention.

Turning now to Figure 8, a process flow diagram of an IP infrastructure set-up procedure according to one embodiment is shown and denoted as 350. Process 350 starts with step 355 wherein the network manager defines one or more domains. Next, in step 360, the manager decides whether or not to define OSPF areas across the

network as shown in step 365. Where no OSPF areas are to be established, process flow is directed to step 370, wherein subnet groups and their masks are established to allow for the full integration of the presently existing network.

The network manager may, at this point, assign administrators, step 375, for domains, networks, OSPF areas, subnet groups and subnets, step 380. Step 380 is essential to preventing unauthorized personnel from accessing the IP data base and attempting to modify or view information about the particular network routing or management scheme in place. Next, the network manager may define Bootp or DHCP servers, step 385, and, if so, setup administrator boundaries, step 390.

At this point, the option of requiring specific vendor extensions is decided, step 395, and if such a requirement is made, the manufacturer's Bootp\DHCP extension is modified and a vendor model template created as shown in step 400.

Alternatively, a set of naming policies can be formulated and assigned to individual platform types as shown in step 405. Process flow is directed to assigning IP addresses to domain primary/secondary servers and

Bootp\DHCP servers in their appropriate subnets as shown in step 410.

Next, in step 415, a migration path within the existing network to the new network topology is started by importing any existing data. If data is imported, it is formatted according to network-wide IP naming policies, step 420, or domain name formats, step 425, or an appropriate local host format, step 430, depending on the nature and type of the imported data.

Where no existing data is imported, the selected IP naming scheme is used to manage all IP hosts and network services as shown in step 435.

An advantageous feature of the improved network architecture according to the invention is its ability to reconfigure network resources from a central upper level of the network hierarchy. This feature is illustrated in Figure 9 in regards to the reconfiguration of DNS addresses and names at various levels of the network infrastructure. Figure 9 is a block diagram showing that the IP manager subsystem 310 updates all primary and secondary DNS addresses following an upper level to lower level migration path. Thus, the primary DNS servers 450 and 455 (redundant systems) obtain DNS updates from the IP manager 310. Likewise, the secondary DNS servers 460

and 465 obtain their updates from the primary servers above 450 and 455.

Where a manufacturer's specific piece of equipment is used and does not conform to established naming policies, the IP manager 310 directly assigns the second DNS server 470. The secondary DNS server 470 can also receive updates from a Non-IP management primary server 475 to permit migration from existing DNS systems to a domain named structure conforming to assigned naming policies.

Another aspect of the improved network architecture according to the invention, is a network management security architecture which ensures confidentiality and integrity of the entire network management architectural layer. In this regard and according to one embodiment of the invention, various layers of security are provided, including personal security, physical security of network components, remote dial-in security, network management security, network operations security and database security.

Figure 10 is a security flow diagram for the network security architecture process 500. As shown, process 500 begins with step 502 when an access request is made which

causes the security access server (AS5200) to perform an authentication table look up step 504. At this point, a point-of-sale (POS) terminal or key operator can be used to verify the validity of the access request, step 506.

Where a POS terminal is used, a radius server is engaged for authentication, step 508, and process flow is directed towards opening a security event audit log, step 514. On the other hand, where the key operator is invoked, the user's specific security token is accepted, step 510. The token, in one embodiment, consists of a personal identification number and a randomly generated access code. The security token is validated, step 512, and, if valid, the event audit log is opened 514.

Where the security token is not valid, the number of attempts is recorded and if the number exceeds a certain threshold, step 516, the user is locked out 518 causing an alarm to be generated, step 520, and an end to the session step 522.

On the other hand, if the user has not reached his attempt threshold, the invalid log attempt is annotated, step 524, and the user prompted for another security token 510. Valid access requests direct process 500 to step 526 wherein the access server is instructed to pass the access request.

Thereafter, process 500 flow is directed to determining if a trusted signal path has been established within an established OSPF path. An invalid path causes a lockout of the user as shown in step 518 while valid path attempts result in the access request being validated, step 530, and the security audit log being closed.

As stated, an advantageous feature of the invention is the centralized configuration of network resources from a single locality. This feature is illustrated in Figure 11 which shows a cabinet 545 version of the core 88 components with approximate dimensions provided according to one embodiment.

Figure 11 has right side components 550 and left side components 560 which comprise the core 88 devices. As shown, a number of routers 562, dial servers 564, and other equipment 566, 568, 570, 572, 574 and 576 can be accommodated in a relatively small space. A back-up router 576 is provided in case a fault occurs.

While this invention has been described and referenced to illustrative embodiments, the description is not intended to be construed in a limiting sense. Various modifications and combinations of illustrative embodiments as well as other embodiments and inventions

will become apparent to those persons skilled in the art upon reference or description. It is, therefore, intended that the pendent claims encompass any such modifications or embodiments.

5

What is claimed is:

1. An architectural hierarchy for a wide area network comprising:

a core network;

a plurality of regional hubs forming a first level of said hierarchy, said regional hubs linked to said core network via a first plurality of data channels;

a plurality of area hubs linked to said regional hubs via an Area 0 signal pathway, said areas hubs comprising a second level of said network hierarchy; and

a plurality of lower level hubs linked to said area hubs via a second plurality of data channels.

2. The architectural hierarchy according to Claim 1 wherein said Area 0 signal pathway is a dual switched Ethernet channel.

3. The architectural hierarchy according to Claim 2 wherein said regional hubs, areas hubs and lower level hubs are routers.

4. The architectural hierarchy according to Claim 3 further comprising:

a first plurality of multiplexers coupled to said

plurality of regional routers;

high speed access paths having first ends and second ends, said first ends extending from said first plurality of multiplexers about one end; and

a second plurality of multiplexers extending to said second ends of said access paths, and providing and entry point into said core network.

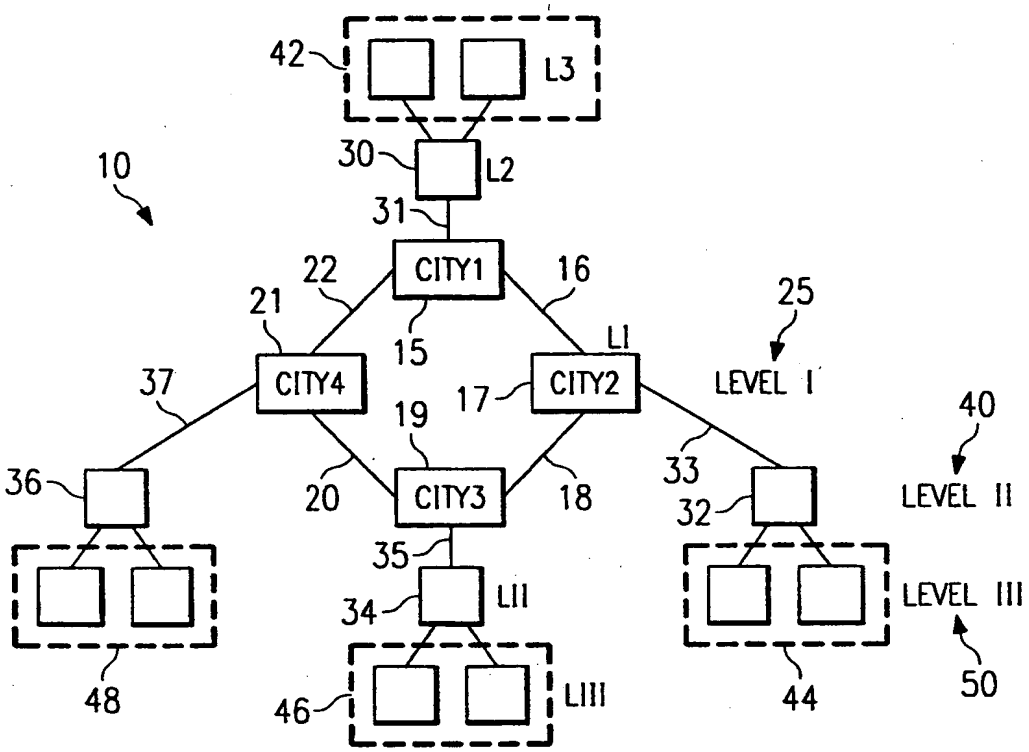


FIG. 1
(PRIOR ART)

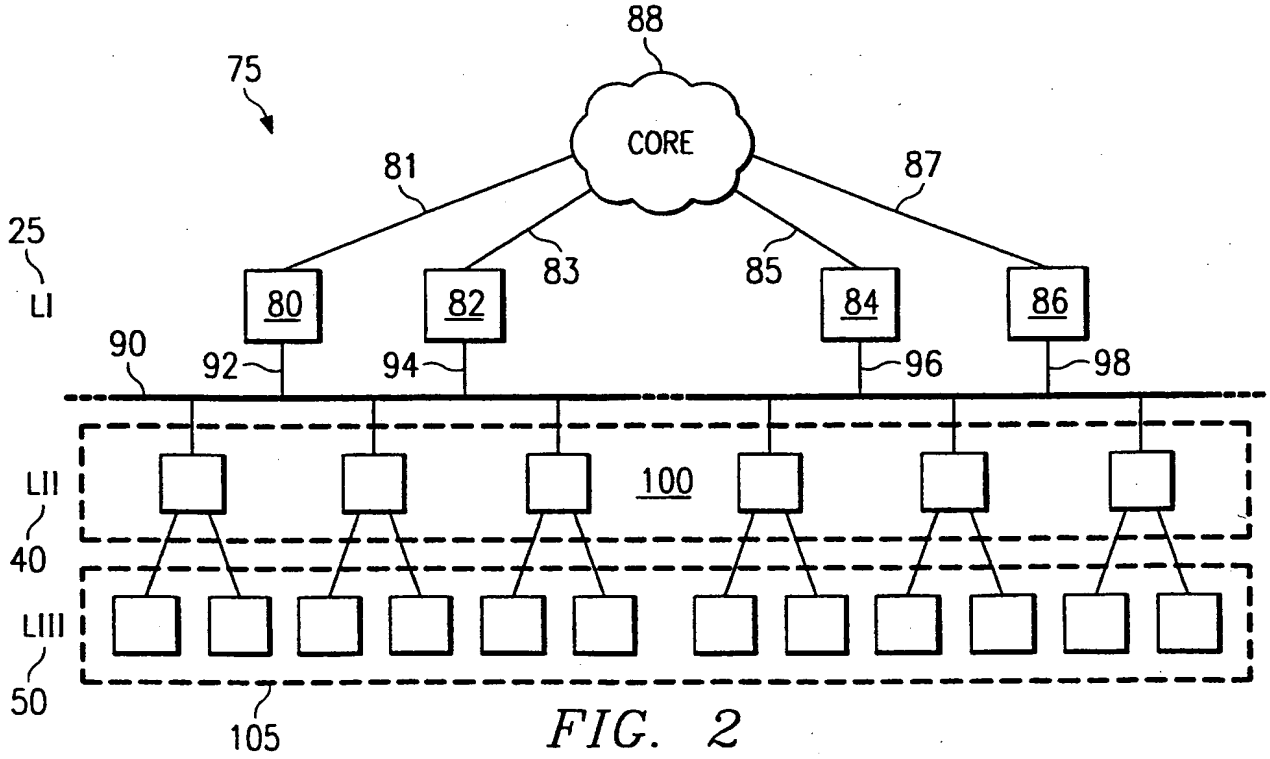


FIG. 2

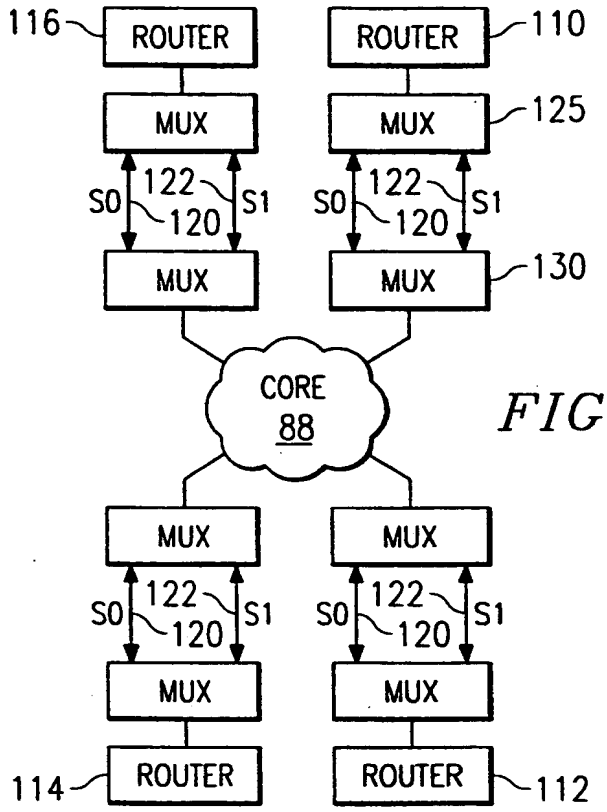


FIG. 3

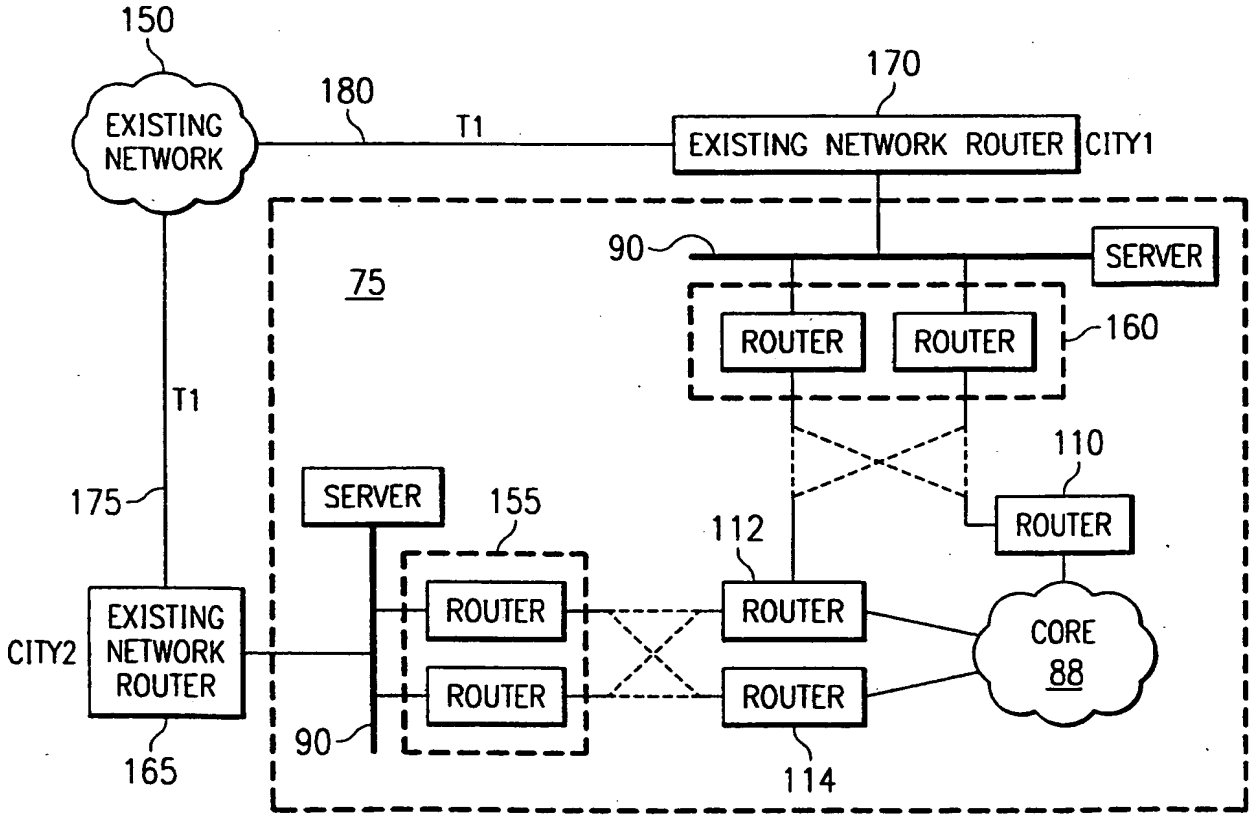


FIG. 4

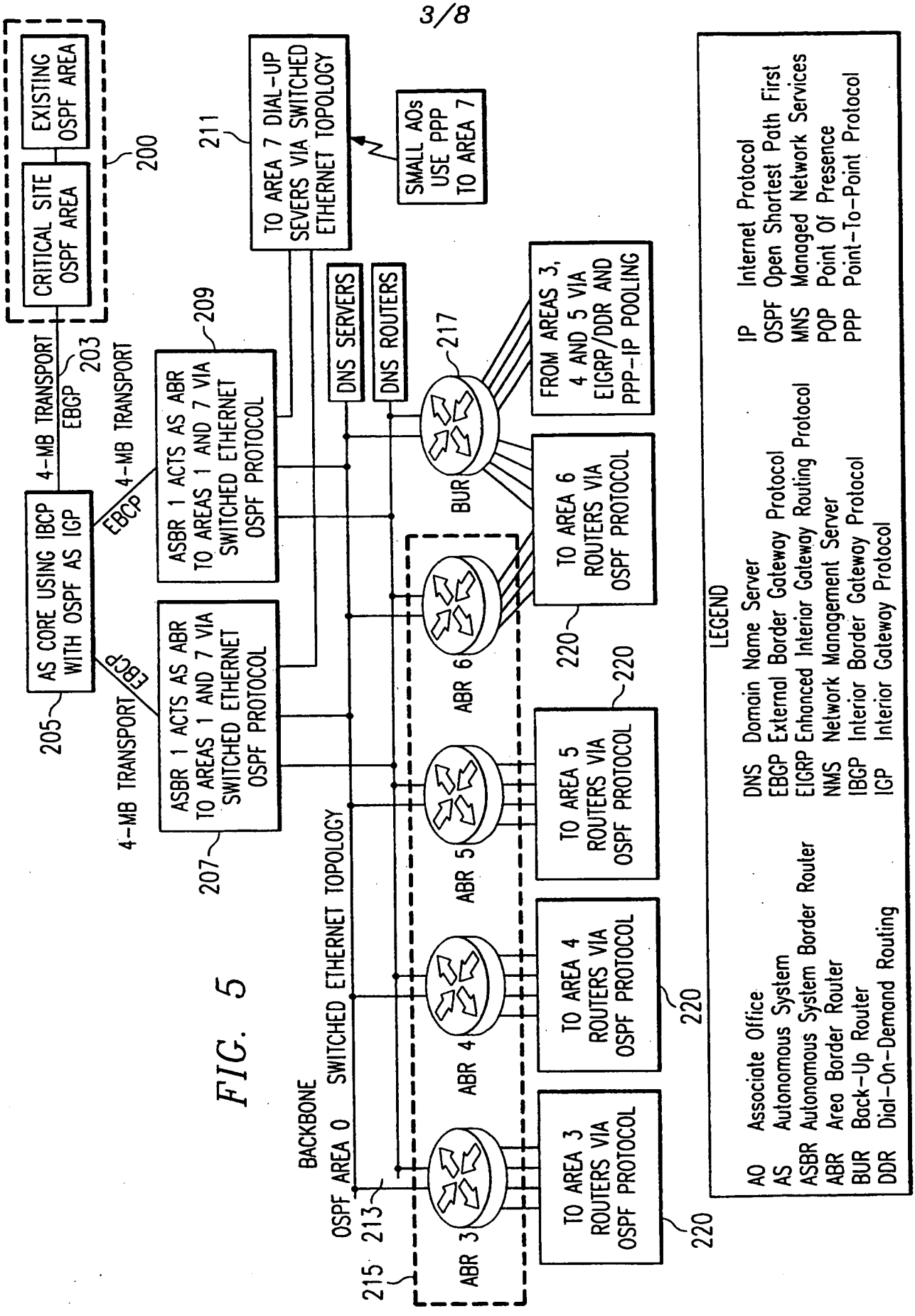
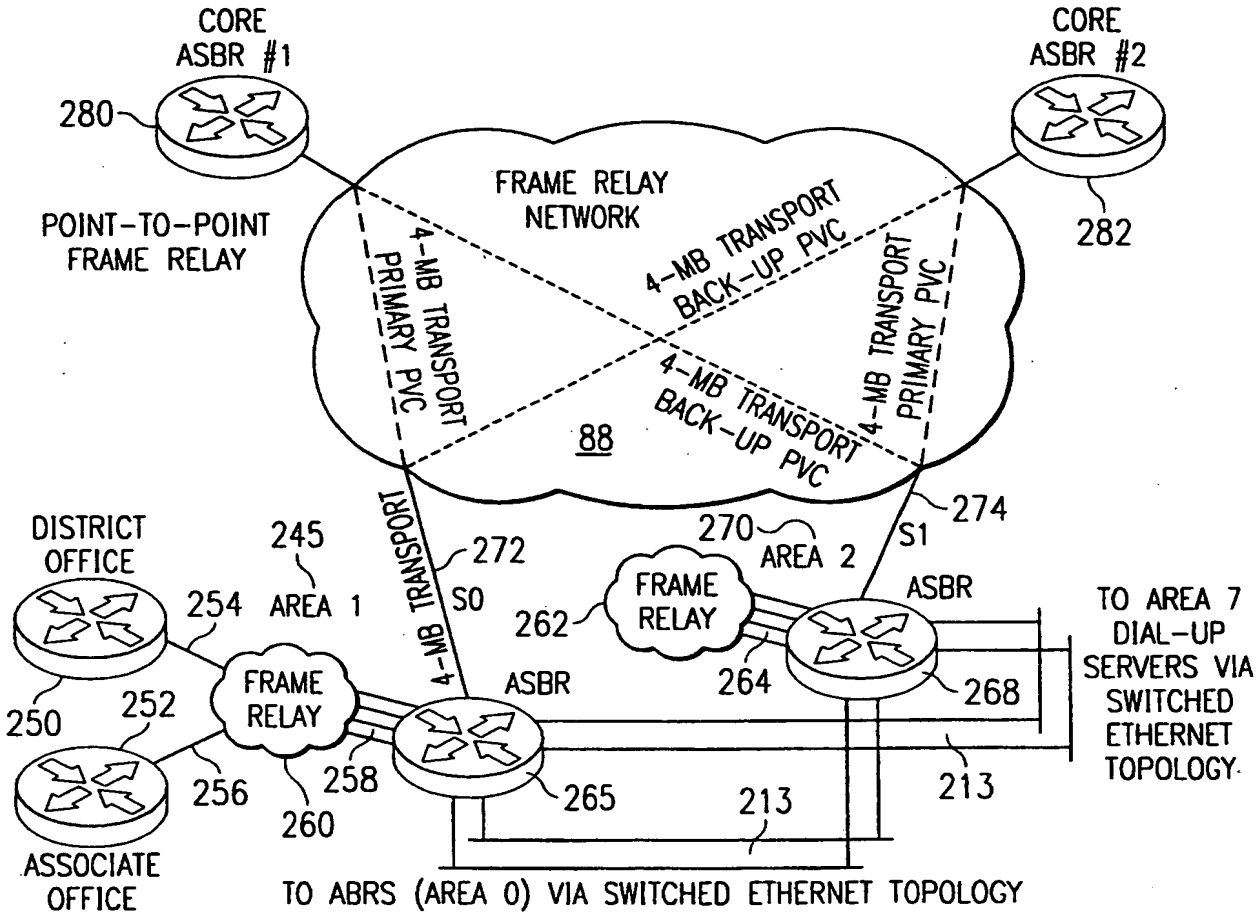


FIG. 5



LEGEND	
ABR	Area Border Router
AO	Associate Office
ASBR	Autonomous System Border Router
DO	District Office
EBGP	External Border Gateway Protocol
POP	Point Of Presence
PVC	Permanent Virtual Circuit

FIG. 6

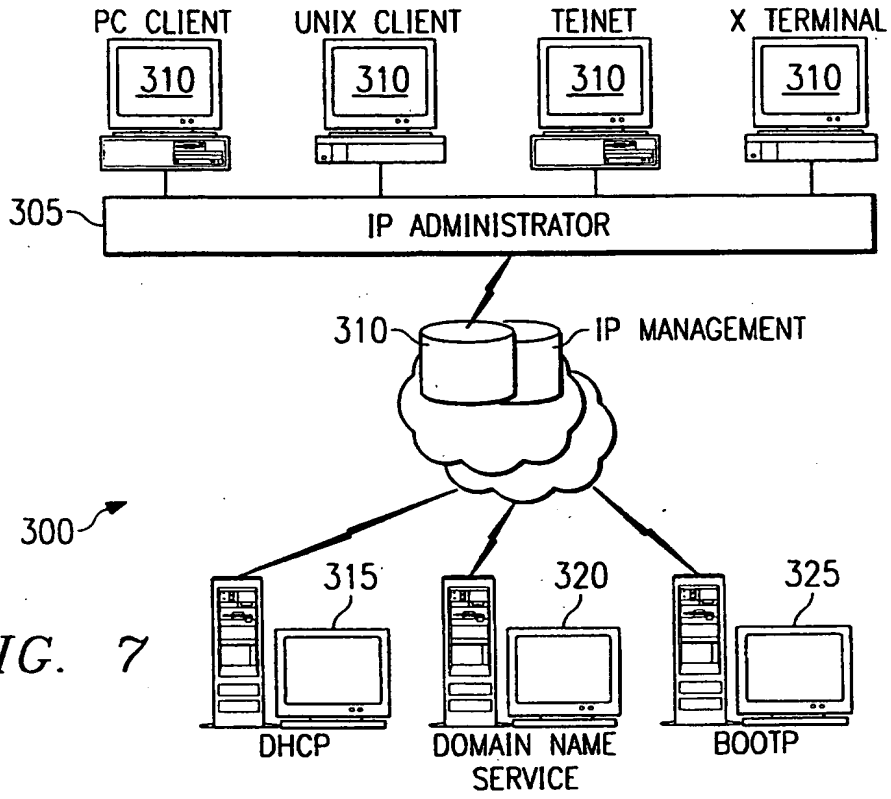


FIG. 7

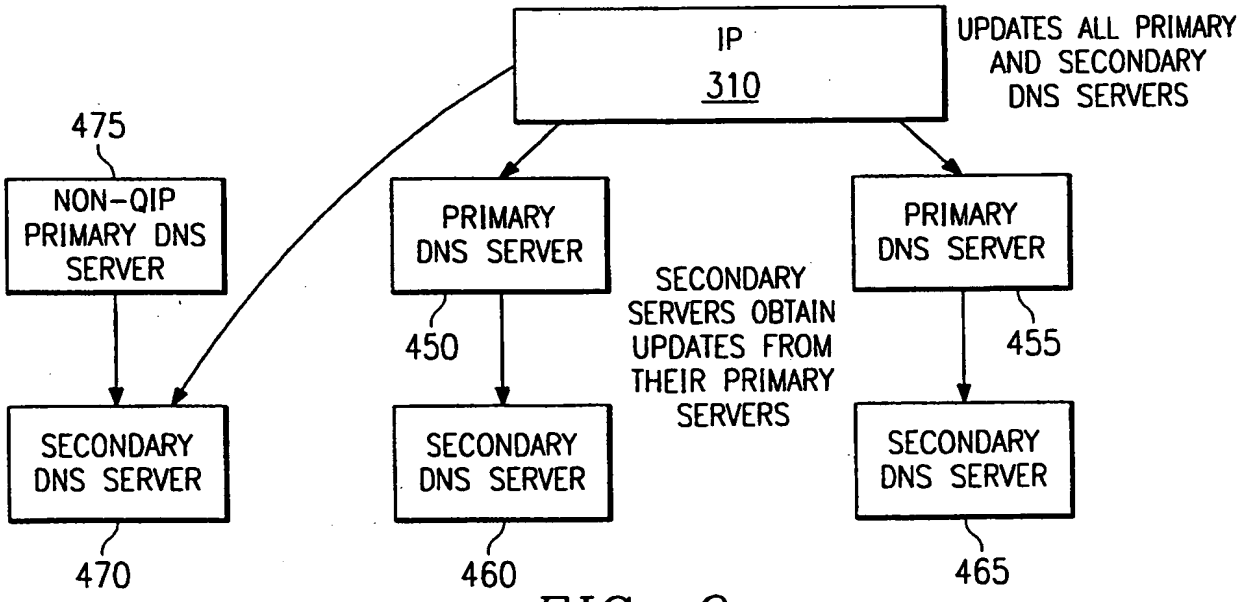


FIG. 9

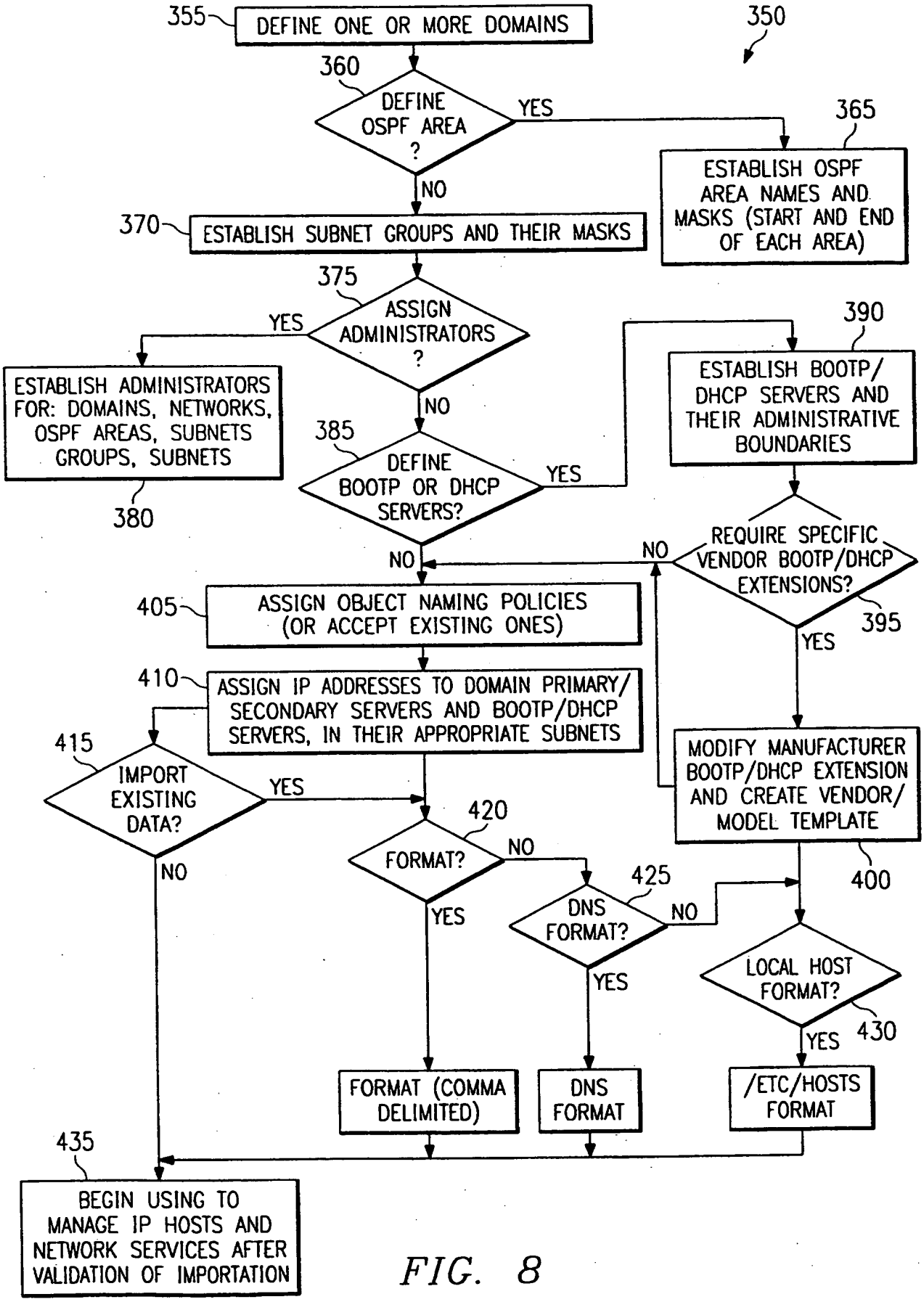


FIG. 8

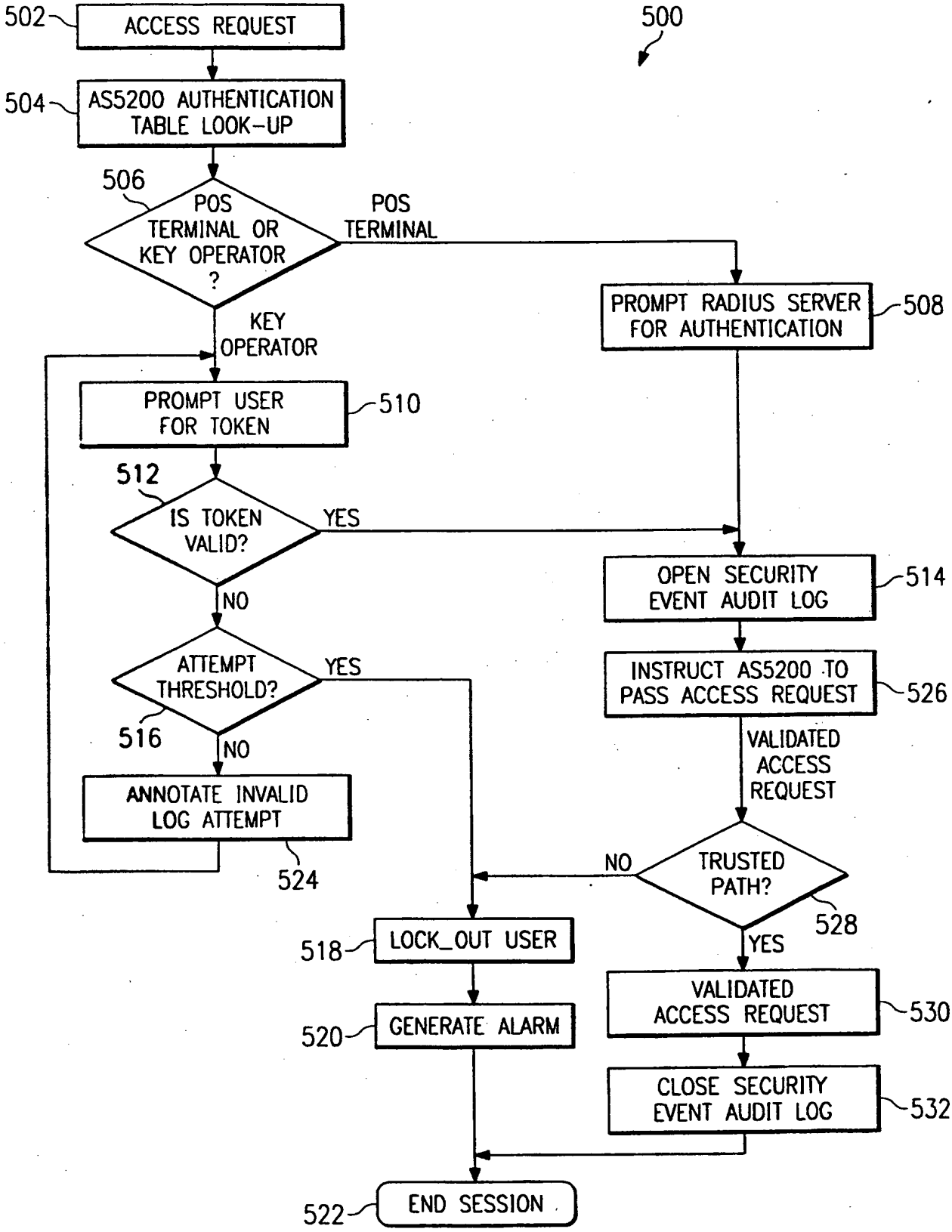
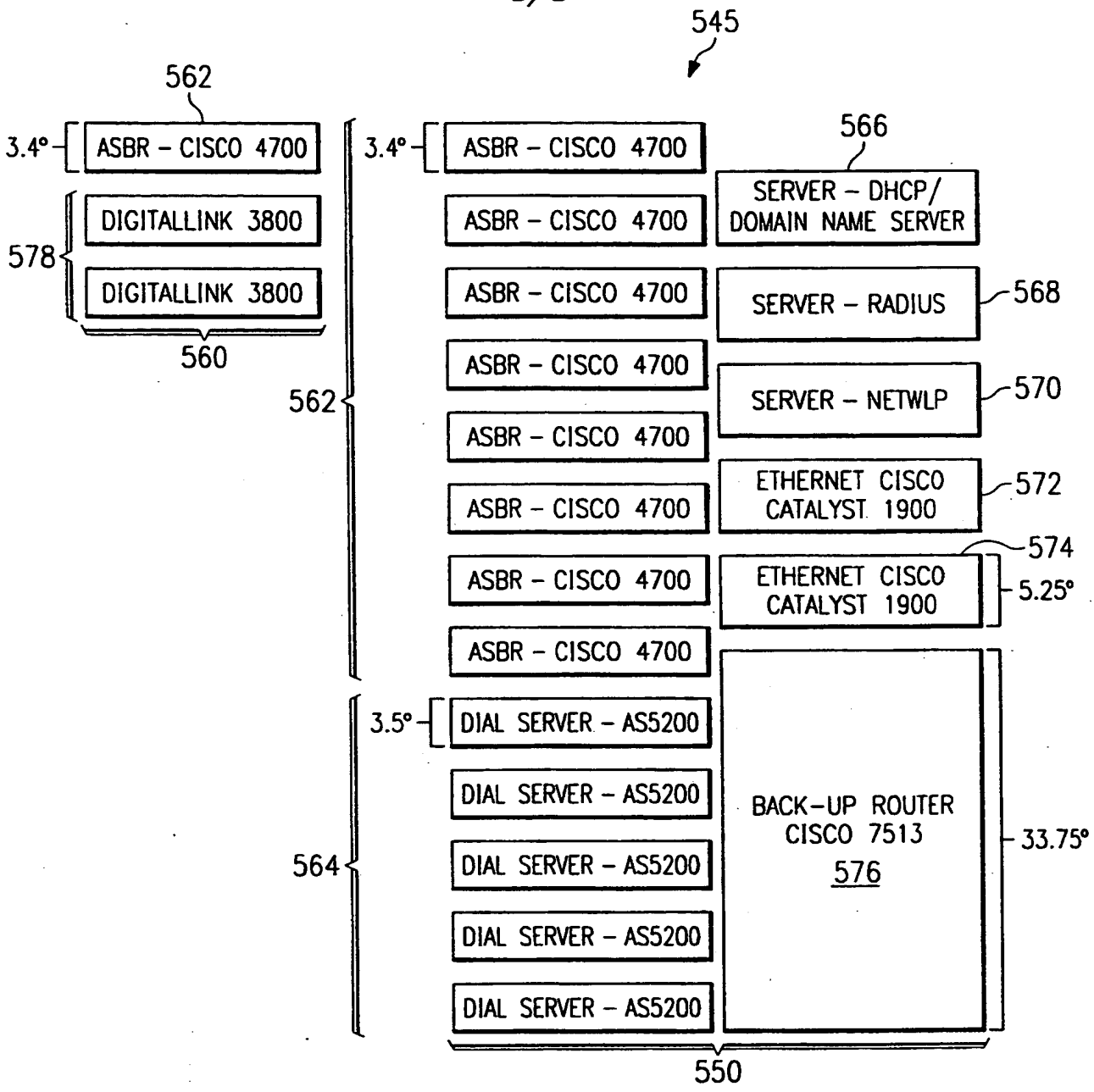


FIG. 10



LEGEND	
ABR	Area Border Router
ASBR	Autonomous System Border Router
ATM	Asynchronous Transfer Mode
CAP	Competitive Access Provider
DHCP	Dynamic Host Configuration Protocol
ISDN	Integrated Switched Digital Network
LEC	Local Exchange Carrier
SMDS	Switched Multimegabil Data Service
SONET	Synchronous Optical Network

FIG. 11

INTERNATIONAL SEARCH REPORT

Int. ational Application No
PCT/US 97/19523

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/46

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	GB 2 283 645 A (DIGITAL EQUIPMENT INT) 10 May 1995 see abstract; figure 1 see page 1, line 1 - page 10, line 11	1 2-4
X A	CLAPP G H: "LAN INTERCONNECTION ACROSS SMDS" IEEE NETWORK: THE MAGAZINE OF COMPUTER COMMUNICATIONS, vol. 5, no. 5, 1 September 1991, pages 25-32, XP000248470 see the whole document	1 2-4

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
10 February 1998	19/02/1998
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Cichra, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. ational Application No
PCT/US 97/19523

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category '	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	EDMONDS C: "PROGRAMMABLE CONTROLLER NETWORKING - DUAL CABLE, REDUNDANCY, MULTIPLE NETWORKS AND APPLICATIONS" ADVANCES IN INSTRUMENTATION AND CONTROL, vol. 47, no. PART 02, 1 January 1992, pages 1411-1423, XP000328967 see the whole document	2-4
A	WO 96 21236 A (CISCO SYSTEMS ;PERIASAMY RAVI (US); CLARK WAYNE (US); PANDIAN GNAN) 11 July 1996 see abstract; figures 1-4 see page 3, line 19 - page 5, line 12 see claims 1-10	1-4
A	MALARA P ET AL: "CLAN AT CRS4: AN EXPERIMENTAL PUBLIC SWITCHED DATA NETWORK" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 25, no. SUPPL. 01, 1 September 1993, pages 17-23, XP000393515	1,2

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ..ional Application No
PCT/US 97/19523

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2283645 A	10-05-95	NONE	
WO 9621236 A	11-07-96	AU 4741896 A	24-07-96

THIS PAGE BLANK (USPTO)